SCIENCE INSTRUMENT AIRWORTHINESS AND CERTIFICATION PROCEDURES MANUAL

Section 500:
Functional Hazard Analysis

500 Functional Hazard Analysis

500.1 Introduction

Each part of the science instrument must be reviewed with associated hazards in mind. Some design parameters are common to each instrument, and have been addressed in other sections of this handbook. This section of the handbook addresses identification of potential hazards, assessment of impact under worst case conditions, i.e. one catastrophic failure, and a risk mitigation plan for bringing any risk down to acceptable levels. Acceptable level of risk implies safety aboard the aircraft to personnel and equipment will not be impacted.

SOFIA must operate under OSHA standards as well as airline safety standards (United Airlines must fly under Federal Aviation Regulations; Part 121, commercial regulations). The manual entitled "Occupational Safety and Health Standards for General Industry" (29 CFR part 1910) is available from http://www.cch.com. This book has safety and hazard analysis and risk mitigation guidelines and is produced by Occupational Safety and Health Administration, United States Department of Labor.

If there are any hazards unique to your instrument that are not addressed in this or any other section of the SOFIA Science Instrument Airworthiness Procedures Manual, you can request further help and advice from the USRA SOFIA Project office, or the SOFIA Science Instrument Airworthiness Integrated Product Team (IPT).

500.2 Functional Hazard Analysis Worksheet

SI teams are responsible for a determination of all hazards associated with their instrument. Begin the FHA by close inspection of system and subsystem design for an idea of which areas will require analysis. Each area of concern will then require an analysis of hazards associated with a worst case failure of that part of the system or subsystem. Identification of latent failures is also required early on in the design. Latent failures are dormant failures within the system that are not inherently revealed at the time the failure occurs. SI teams do not need to consider the possibility of two catastrophic failures at the same time. Use reasonable estimates and do not be overly conservative, accurate calculations are what is required. Note that specifics have been provided in section 300 and 400 on the mechanical and electrical analysis.

500.2.1 FAA Functional Hazard Analysis Worksheet

When a thorough analysis of the science instrument has been completed, it is necessary to summarize the results for utilization by the FAA for flight certification. The required format for this spread sheet is shown in figure 502-1 and includes the system identification and instrument name as well as the columns as follows:

Column 1: Function

Describe what purpose is served by the identified system (or subsystem)

Column 2: Hazard Description

Discuss what potential safety hazard might exist and what circumstances could cause the hazard.

Column 3: Phase

List the appropriate code(s) for when the hazardous condition could exist. The hazard may exist during all phases. Phases are:

Ground = G
Taxi = T
In Flight = F
Landing = L

Column 4: Effect on Aircraft or Personnel:

Describe the worst case effects such as damage to A/C, injury or death to personnel

Column 5: Failure Condition

The Federal Aviation Regulations or Government Regulation, which describes the failure condition.

Column 6: Category of Effects

Evaluation of data will indicate which category most accurately describes the potential hazard. Categories include:

Catastrophic: Catastrophic failure conditions must be extremely improbable, there have been either crew fatalities or crew incapacitation, there have been multiple passenger fatalities and the aircraft is normally a loss. The allowable quantitative probablity is less than 1E-9.

Hazardous: Hazardous failure conditions must be extremely remote, there has been physical crew distress or excessive workload impairs crew ability to perform tasks, there has been serious or fatal injury to a small number of passengers and there is a large reduction in aircraft functional capabilities or safety margins. The allowable quantitative probability is less than 1E-7.

Major: Major failure conditions are remote, there has been physical crew discomfort or a significant increase in crew workload, there has been physical distress to the passengers (possibly including injuries) and there is a significant reduction in aircraft functional capabilities or aircraft safety margins.
The allowable quantitative probability is less than 1E-5.

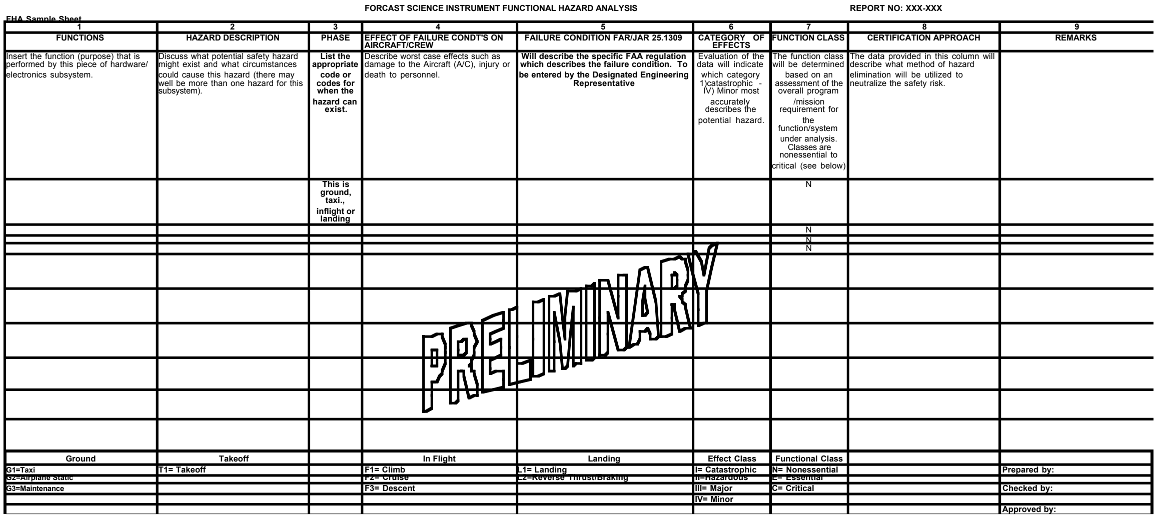
Minor: Minor failure conditions are probable, there has been a slight increase in crew workload or use of crew emergency procedures, there has been physical discomfort for passengers and there is a slight reduction in aircraft functional capabilities or aircraft safety margins. The allowable quantitative probablity is less than 1E-3.

Column 7: Function Class
This will be determined based on an assessment of the overall program or mission requirement for the function or system that is analyzed in this particular spread sheet. In general, NOTHING on the science instrument side is essential for flight (exceptions include the pressure boundary in some cases). The function classes are;

N = Nonenssential (Science Instrument)
E = Essential
C = Critical

Column 8: Certification Approach
Data provided in this column will describe what method(s) will be utilized to neutralize the hazard.

Column 9: Remarks.



FHA Sample Sheet

FORCAST SCIENCE INSTRUMENT FUNCTIONAL HAZARD ANALYSIS

REPORT NO: XXX-XXX

1	2	3	4	5	6	7	8	9
FUNCTIONS	HAZARD DESCRIPTION	PHASE	EFFECT OF FAILURE CONDT'S ON AIRCRAFT/CREW	FAILURE CONDITION FAR/JAR 25.1309	CATEGORY OF EFFECTS	FUNCTION CLASS	CERTIFICATION APPROACH	REMARKS
Insert the function (purpose) that is performed by this piece of hardware/ electronics subsystem.	Discuss what potential safety hazard might exist and what circumstances could cause this hazard (there may well be more than one hazard for this subsystem).	**List the appropriate code or codes for when the hazard can exist.**	Describe worst case effects such as damage to the Aircraft (A/C), injury or death to personnel.	**Will describe the specific FAA regulation which describes the failure condition. To be entered by the Designated Engineering Representative**	Evaluation of the data will indicate which category 1)catastrophic - IV) Minor most accurately describes the potential hazard.	The function class will be determined based on an assessment of the overall program /mission requirement for the function/system under analysis. Classes are nonessential to critical (see below)	The data provided in this column will describe what method of hazard elimination will be utilized to neutralize the safety risk.	
		This is ground, taxi., inflight or landing				N		
						N		
						N		
						N		
Ground	Takeoff		In Flight	Landing	Effect Class	Functional Class		
G1=Taxi	T1= Takeoff		F1= Climb	L1= Landing	I= Catastrophic	N= Nonessential		Prepared by:
G2=Airplane Static			F2= Cruise	L2=Reverse Thrust/Braking	II=Hazardous	E= Essential		
G3=Maintenance			F3= Descent		III= Major	C= Critical		Checked by:
					IV= Minor			
								Approved by:

Figure 500.2-1 FAA failure analysis format. The columns are detailed in the appendix with examples of this type of analysis.

500.2.2 NASA Ames Research Center Forms

Because the SOFIA project is a NASA program, it may be required that science teams include the NASA hazard form in the final documentation package. This is not an FAA requirement. The material and information required on the NASA form is similar to that on the FAA form above, but some of the definitions are slightly different. The forms and instructions are included in Appendix V of this manual.

500.3 Cryogen Limits

Cryogen volume allowed to ensure oxygen content in SOFIA aircraft must not fall below acceptable levels (19.5%) under worst case conditions. The only cryogens that will be allowed aboard SOFIA at this time will be liquid helium and liquid nitrogen. The safe amounts, based on SOFIA cabin volume of 36,000 cubic feet, are;

Liquid Helium 70 liters (TBC)
Liquid Nitrogen 70 liters (TBC)

These limits are set by the hazards associated with a catastrophic failure of the science instrument. A catastrophic failure includes for example, loss of cryostat vacuum due to a window failure, that raises the loads on the cryogen reservoir enough to boil off all the helium in short time (a couple of minutes). The aircraft cabin oxygen must remain above a limit of 19.5%. (OSHA standard). An example of this type of calculation is in Appendix II. Note that these calculations are not concerned with the standard boil off loads associated with the cryogen volume, as these are not enough to create a hazard.

500.4 Mechanical Guidelines

This section should address all areas of concern to your particular instrument. For example, if your internal supports should fail, what would be the result? Could the external vacuum keep the damage internal to the cryostat and not impact safety? Also include catastrophic failure modes (instantaneous loss of vacuum, window breakage o-ring failure etc.)

Internal Mechanical systems failures include G-10 supports breaking, optics bench not secured. A quick calculation of internal weight and structural integrity of the outer vacuum jacket will suffice here, and since most instruments are designed for stiffness, these types of failures should not pose a safety hazard. Please refer to the mechanical certification guidelines, Section 300, in this manual for additional information and examples of analysis.

500.4.1 Worst Case Failure Modes for a Cryostat

This document is intended to explain the failure modes for a fairly simple cryostat. The numbers presented are order of magnitude calculations generally erring on the side of safety. In describing the failure modes in an FAA document, each instrument team would need to make more detailed analysis and calculations for their particular cryostat. The following sections are an example of a hazard analysis for a simple cryostat.

500.4.1.1 Cryostat Description

In general, cryostats are composed of one or two liquid cryogen reservoirs within a vacuum jacket. There are more complicated systems, but for the purpose of this document, we will consider a basic system with a liquid nitrogen (boiling temperature of 77K) and a liquid helium (boiling temperature 4K) reservoir (see Figure 5). The temperature of the experiment is maintained by the boiling of these cryogens. The primary safety issues unique to cryostats are associated with the gaseous helium.

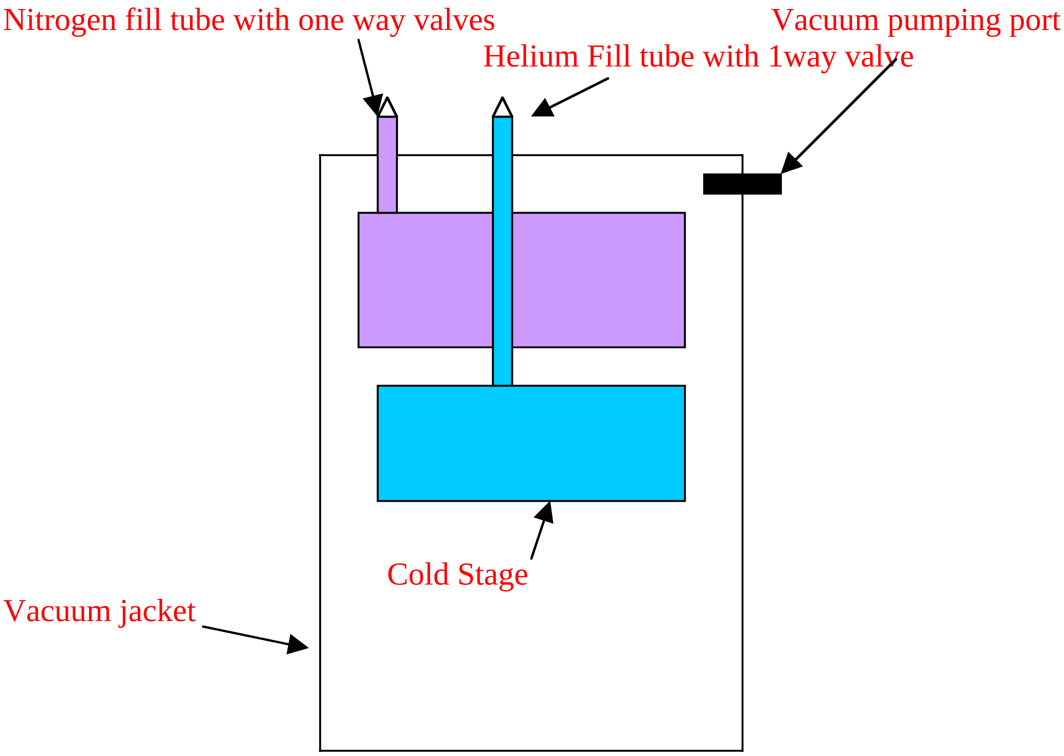

Nitrogen fill tube with one way valves
Vacuum pumping port
Helium Fill tube with 1way valve
Cold Stage
Vacuum jacket

Figure 500.4-1 Simple Cryostat with cryogen reservoir

In normal operation, cryogen boil-off will be quite small. A ground-based system might boil 5 liters of LHe and 5 liters of LN_2 in 24 hours. Note that the heat loads on the LN_2 are typically on the order of 10 W while the LHe heat load is on the order of 100 mW. It is because LN_2 requires considerably more energy to boil than LHe that the primary safety concerns are associated with the helium. A rough number for converting liquid cryogen volumes to room temperature and pressure (RTP) gas volumes is to multiply the liquid volume by 750. This is the correct factor for LHe while LN_2 has an expansion factor of 700. Therefore, the system described above boils roughly 0.06 cm^3 of each liquid per second. If this gas escapes the fill tubes at RTP, it would have a flow rate of 45 cm^3/sec for LHe and 42 cm^3 for LN_2. Although the escaping gas, known as boil-off, is colder than room temperature, assuming RTP is likely to at most a 20% overestimate. For a neck tube with a 1 cm^2 cross-section, the flow velocity is 1 mph.

The boil-off is directly related to the thermal energy deposited into the cryogen volume. Maintaining a vacuum in the cryostat minimizes gaseous conduction. In most cases, the dominant heat load on the liquid nitrogen is radiation from the room temperature outer jacket, while conduction through mechanical structures is the dominant load on the helium. To minimize radiation, reflective material such as aluminized mylar layers are inserted between different temperature surfaces. To minimize conduction, fiberglass is frequently used for structural support, electrical wires are thin, and cryogen reservoir fill tubes are thin walled stainless steel.

500.4.2 Failure Modes

For the purposes of this example, two failure modes will be discussed. One, blockage of the boil-off venting that causes an overpressure in a cryogen reservoir and two, failure of a structural component that creates a dramatically increased heat load.

500.4.2.1 Neck Tube Ice Plug

An ice plug can form in the neck tube of a cryostat when air enters the tube and freezes. Ice plugs are much more common in LHe fill tubes because the colder temperatures mean air entering the fill tube can freeze to form the plug. Water condensation dripping down the LN_2 fill tube is required to form an ice plug and is extremely rare.

Ice plugs can be avoided by methods such as installation of a one-way valve at the input of a fill tube so that only the cryogenic gas will be in the fill tube. This will prevent back flow of air into the fill tube, and prohibit ice plug formation. By monitoring the boil-off rate, typically done simply by looking at the amount of vapor coming from the fill tubes, an experimenter can immediately determine that there is no ice plug. In the airplane environment, ice plugs are most common when descending from altitude into humid air, but can be completely eliminated by placing a one-way valve on all the vent/fill tubes.

In the event of an ice plug, the pressure in the helium cryogen reservoir will build. This change in pressure is not immediate; but gradual. The gas within the reservoir will likely remain reasonably cold until the liquid is gone. Ice plugs will not generally cause a significant increase in the heat load on the LN_2 cryogen can. Thus, having an ice plug in one cryogen neck does not result in dramatically increased boil-off from the LN_2.

500.4.2.2 Ice Plug Prevention

In order to prevent ice plugs, each cryogen reservoir will be required to have either a coaxial neck insert, a double neck on the cryogen reservoir or a cryogenic relief disk on the reservoir. While these three choices will satisfy the requirement for safety, the coaxial neck tube has the advantage of easy use, reliability and low cost. Science instrument builders may choose to use the cryogenic relief devices, but the cost of engineering and manufacture may be prohibitive (information on these cryogenic relief devices is available in Appendix III (resources)).

The specifics of the design are at the discretion of the science instrument builder, but a concept design as depicted by the FIFI-LS team is shown in Figure 505.2-1. Several options for this safety device have been reviewed within the IPT for optimum performance and reliability, the best choice seems to be a coaxial neck tube placed in each cryogen neck after filling.

500.4.2.3 Vacuum Jacket Safety

It is simple to add a low-pressure relief disk onto the vacuum jacket. As the vacuum jacket is pumped out (i.e. internal pressure $\sim 10^{-4}$), a small disk (1" diameter or so) on the side of the vacuum jacket can be mounted to be leak tight. However, if the differential pressure across the disk becomes zero (as would be the case if there were a vacuum failure), the disk would simply fall off. In this case, there is no chance for pressure to build inside the vacuum can. The small (1" or so) disk can be mounted with a lanyard such that when it does fall off it is held close to the vacuum can and does not cause a hazard.

500.4.2.4 Structural Failure

From a thermal standpoint, the worst structural failure of a cryostat is a sudden loss of vacuum in the cryostat outer vacuum jacket. Likely scenarios for this include failure of the window to the cryostat, breaking a feed through such as a pumping port, accidental opening of a vacuum pumping port, and breaking of the neck tubes because of some large shock. Most of these failures would involve dropping the cryostat, which would not occur in flight. The window could conceivably be cracked by pressure induced from thermal contraction upon exposure to the telescope cavity, although unlikely since the temperature of the window and its surrounding material will be close to the same temperature. The window could possibly be damaged if focused sunlight is allowed to land on its surface. The probability of any of these things occurring is very low.

A failure of the vacuum jacket means that gaseous conduction is now an effective means of heat transfer into both the LHe and the LN_2. The heat load on the LHe increases by four orders of magnitude whereas the LN_2 increase is a factor of 50. The boil-off rates are proportionally larger. For the case imagined above, the 5 liters of LHe would be boiled in 10 s. Because of the much higher heat capacity of the liquid nitrogen, it would take over 30 minutes to boil away.

This increased boil-off would be venting out the fill tubes unless the structural failure involved the fill tubes. For a broken vacuum jacket (caused by a broken window or pumping port), the cryogen reservoir and boil-off path are still undamaged at this point. Using the factor of 750 given above, the 5 liters of LHe would produce 3750 liters of RTP He (3.75 cubic meters. Note that if the hole in the cryostat opened to the telescope cavity (such as a broken window), the boil-off would be escaping into the cavity. Conversely, if the hole were in the cabin, the boil-off would be venting into the cabin.

If a 5 liter LHe dewar had a cylindrical vacuum jacket with dimensions 0.5 meter diameter and 0.75 meter height, it would have a volume of 0.15 cu meters. Given that the RTP volume would be 3.75 cubic meters, the pressure in the vacuum jacket (neglecting the LN_2 since it takes so much longer to boil) would be 25atm. Analysis shows that most cryostats built for stiffness are probably capable of holding such a pressure (see analysis in Section 300, Mechanical)

500.4.2.5 Cryogenic Relief Devices (Burst Disk)

While a cryogenic temperature relief device has been identified that may be suitable for use in SOFIA science instruments, the cost and technical risk involved will prohibit generic relief disk development within the SOFIA project. Science instrument builders preferring to use a cryogenic relief device must therefore bear the cost and risk of development and manufacture of this device. The burst disk (made by Hydrodyne Inc.) has been used on Gravity Probe B in a superfluid helium cryostat with reliable results. Preliminary analysis of sizing and throughput will be done and provided to teams wishing to develop such a relief device.

500.4.3 Conclusions

The probability of a cryostat failure is very low, but we must consider the possibility in the interests of safety. For a typical cryostat, the major safety concern is the liquid helium cryogen. The two failure modes for cryostats are ice plugs that block normal venting of boil-off and a loss of vacuum that causes greatly increased thermal load on the cryogen volume. Steps can be taken to minimize the likelihood of failures such as one-way valves on cryogen vent lines and safe handling procedures. It has been shown that catastrophic failure of the cryostat does not result in a hazardous condition in the aircraft.

500.5 Electrical Guidelines

Electrical systems should be designed to eliminate hazards, still a short analysis of possible failure modes and what safety impact they might have will be required. There may be no safety impact, but that can be stated also. Obvious hazards include the use of high voltages or currents and these can be mitigated by using proper sizing of fuses or automatic shut off in case of a failure. Please refer to the electronics certification guidelines (Section 400) in this manual for further information.

500.6 Cryostat Subsystem Failure Modes

500.6.1 Calibration Gas Example

The amount of gas allowed will depend on OSHA standard volume exposure limits in parts per million (ppm). If using a particular type of gas, you must determine that a catastrophic failure would not impact safety on board the aircraft. Gas containment in cylinders must include a plan for holding the cylinders in place on the aircraft in such a way that it will not impact safety from any aspect. This includes temperature concerns, safety and security of mounting, and perhaps containment in a box or other enclosure depending on risk assessment. Note that this hazard assessment is based on amount used during KAO operations (NASA Ames Research Center SOFIA Project Office)

Along with your hazard analysis you should keep copies of Material Safety Data Sheets (MSDS) as part of your certification documentation for all gases that may be used.

500.6.1.1 Example of a Hazard Calculation:

Anhydrous Hydrogen Chloride (Worst Case Hazard). *Worst case assumes instantaneous rupture of the calibration gas cylinder, releasing all contents into the cabin. This can happen if a cylinder is knocked or dropped such that the cylinder head is cracked. Probability: Low

Assumptions:

SOFIA volume	36,000 ft3
Volume of HCL gas in cylinder	X in ft3

Concentration Calculation

Concentration = Volume in cylinder/Volume of SOFIA cabin = X/70,000. For this example, we use a typical value of X for a KAO cylinder of 5.3 cubic feet, which gives a concentration of 75 ppm for this particular example. As shown in the next section this is over an order of magnitude higher than the long term exposure level allowed by OSHA standards for HCL.

OSHA/ MSDS Standards for HCL:

1) 5ppm	long term exposure level (8-12 hours)
2) 10ppm	5 min., 8 times over 8 hours
3) 100ppm	Immediate danger level hazard

500.6.1.2 Conclusions:

Safe amount for HCL would give a concentration less than 5 ppm, the long term exposure level shown above and this determines the value of X. In this case the safe volume of HCL would be 5 x10^{-6} * 36,000= X = 0.18 cubic feet. This calculation indicates that a cylinder carrying HCL will be safe if carrying less than 0.18 cubic feet of this particular gas.

500.6.2 Example Hazard Analysis for Hydrogen Chloride (standard operations)

Analysis for momentary concentration levels during routine calibration procedures. This procedure releases about 10^{-3} ft3 of the gas during calibration. Most is injected into the instrument, but if allowed to escape would result in release of 0.03 ppm of the gas and is not a safety hazard for either personnel or aircraft. Probability of this happening can be several times per science flight.

500.6.2.1 Conclusion

Standard operation use of anydrous HCL is safe.

500.6.3 Hazard Listing

List hazards associated with the particular gas you plan to use. An example for Anhydrous Hydrogen Chloride follows.

500.6.3.1 Properties:

Anhydrous Hydrogen Chloride is a colorless gas which fumes strongly in moist air and has a highly irritating effect on the body tissues. It has a sharp, suffocating odor. Chemically, the hydrogen chloride is relatively inactive and non-corrosive in the anhydrous state. However, it is readily absorbed by water to yield the highly corrosive hydrochloric acid, in this state it can react rapidly, with many organic substances. The concentration level of 5 ppm should not be exceeded during any part of the working day.

500.6.3.2 Physiological effects:

Inhalation of excess quantities of hydrogen chloride gas produces coughing, burning of the throat, and a choking sensation. Occasionally, ulceration of the nose, throat, larynx, or edema of the lungs has resulted. Prolonged inhalation of high concentrations may cause death. The irritating character of these vapors provides a warning of dangerous concentrations well before injury can result. Concentration of 50 ppm cannot be tolerated for more than an hour and concentration of 1500-2000 ppm are fatal within a few minutes. Repeated exposure of the skin to concentrated anhydrous hydrogen chloride vapor may result in burns or dermatitis.

500.7 Conclusion

This section has included several different examples of hazards associated with the science instruments. However, a specific SI should include analysis of all hazards associated with your instrument that have not been addressed in any other part of the above. If you are using a laser for example, then you must document the type of laser and associated hazards. Also, some failure modes, and associated risk with those failure modes must be listed. For example, if the laser fails to operate this would not impact safety at all, but if an interlock fails (no need to analyze double failure modes) you should identify all possible problems associated with that failure such as danger to personnel or equipment.